AO 106 (Rev. 04/10) Application for a Search Warrant (Modified: WAWD 10-26-18)

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

One Apple iCloud Account

Case No. MJ20-516

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

The Apple iCloud account described in Attachment A, incorporated by reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 844(f)(1) and (i)	Arson

The application is based on these facts:

✓ See Affidavit of FBI Special Agent Nathan Plough, continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

Nathan Plough, FBI Special Agent
Printed name and title

○ The foregoing affidavit was sworn to before me and signed in my presence, or
◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 08/11/2020

Judge's signature

City and state: Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge
Printed name and title

USAO# 2020R00533

ATTACHMENT A

Apple iCloud Account to be Searched

The electronically stored data, information and communications contained in, related to, and associated with (including all preserved data) the Apple iCloud account associated with the following Apple user identifiers:

- The email account yaherd300[@]gmail.com, and digital sign identifier 16913302770 ("SUBJECT ACCOUNT");

as well as all other subscriber and log records associated with the SUBJECT ACCOUNT, which are stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cuptertino, California. Brackets have been placed in the name and/or identifiers of the SUBJECT ACCOUNT to ensure that it is not inadvertently hyperlinked and contacted.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

I. Information to be disclosed by Apple for search

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government for the SUBJECT ACCOUNT listed in Attachment A, **within fourteen (14) days of the issuance of this warrant**:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address(es) used to register the accounts, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the accounts (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, Bookmarks, Contacts, Safari Browsing History, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

i. All records pertaining to communications between Apple and any person(s) regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

I. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of Title 18, United States Code, Sections 844(f)(1) and (i) (Arson) for the SUBJECT ACCOUNT listed on Attachment A, for the time period May 1, 2020, through August 11, 2020, including:

a. Content that serves to identify any person who uses or accesses the SUBJECT ACCOUNT, or who exercises in any way any dominion or control over the account;

b. Content, including but not limited to communications, photographs, or videos that depict or describe the arsons under investigation that took place on May 30, 2020;

c. Content that constitutes communications relating to the crimes set out above;

d. Content that evidences the state of mind of any person(s), including the user(s) of SUBJECT ACCOUNT, with regard to the crimes set out above, including but not limited to communications, photographs, and videos relating to protests taking place in Seattle, Washington and elsewhere during May through August 2020;

e. Content that may reveal the current or past location of the individual or individuals using the SUBJECT ACCOUNT;

f. Content that may reveal the identities of and relationships between co-conspirators with regard to the crimes set out above;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

g. Content that may identify any alias names, online user names, "handles" and/or "nics" of those who exercise in any way any dominion or control over the SUBJECT ACCOUNT as well as records or information that may reveal the true identities of these individuals;

h. Other log records, including IP address captures, associated with the SUBJECT ACCOUNT;

i. Subscriber records associated with the SUBJECT ACCOUNT, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, Including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Apple in relation to the account; 6) account log files (login IP address, account activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

j. Records of communications between Apple and any person purporting to be the account holder about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

The requested warrant authorizes a review of electronic storage media, electronically stored information, communications, and other records and information seized, copied or disclosed pursuant to the warrant in order to locate the evidence described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Nathan Plough, having been duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

I am a Special Agent with the Federal Bureau of Investigation (FBI). I have been a Special Agent with the FBI for approximately two and a half years. I am currently assigned to the Seattle Field Office where I am assigned to investigate domestic terrorism matters.

During my service with the FBI, I have investigated and participated in the investigations of criminal activity, including but not limited to: crimes against persons, crimes against property, and conspiracy against civil rights. During these investigations, I have participated in the execution of search warrants and the seizure of evidence indicating the presence of criminal violations. As an FBI Agent, I have also conducted or participated in physical surveillance, debriefings of informants, and reviews of records and recordings. I have also managed undercover operations. From these experiences, and from related training, I have become familiar with the ways in which persons coordinate, carry out, and conceal criminal activity. During past investigations, I have also participated in the execution of search warrants and the seizure of evidence indicating the presence of criminal violations.

The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement personnel; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

PURPOSE OF AFFIDAVIT

I submit this affidavit in support of an application under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), for a search warrant for information associated with the following account: The Apple iCloud account registered under the email account yaherd300@gmail.com, bearing digital sign identifier 16913302770 ("SUBJECT ACCOUNT"), which is stored at premises controlled by Apple, Inc., an electronic communications service and remote computing service provider headquartered in Cupertino, California.

The information to be searched is described in the following paragraphs and in Attachment A. The warrant would require Apple to disclose to the government copies of the information (including the content of communications) relating to the SUBJECT ACCOUNT, as further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review this information to locate the items described in Section II of Attachment B.

The requested warrant would authorize a review of electronic storage media, electronically stored information, communications, and other records and information seized, copied or disclosed pursuant to the warrant in order to locate the evidence described in this warrant. The review of this electronic data would be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI would be permitted to deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 844(f)(1) and 844(i) (Arson) have been committed by Kelly Jackson, and that evidence of those violations will be found in the SUBJECT ACCOUNT.

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

SUMMARY OF PROBABLE CAUSE

A. The Arsons of Seattle Police Department Vehicles on May 30, 2020.

On May 30, 2020, there was a large protest in the downtown area of Seattle, Washington. Seattle Police Department (SPD) officers and other employees were in the area to direct traffic and ensure the safety of people and property. SPD officers and employees used several vehicles to respond to the protest, including the following vehicles:

Vehicle 1: A 2018 Ford Transit Connect van owned by SPD and assigned to the Video Unit. This van was not marked as a police vehicle, but was equipped with a police radio and flashing strobe lights. The SPD Video Unit employees used the van for transportation, to record videos of particular locations and events, and to download surveillance video provided by local businesses and residences in support of SPD criminal investigations. During the protest on May 30, 2020, SPD used and intended to use the van for transport and to document acts of violence and property destruction. Vehicle 1 was parked on 6th Avenue between Pine Street and Olive Way.

Vehicle 2: A 2006 Dodge Caravan owned by SPD and assigned to the Video Unit. This van was not marked as a police vehicle, but was equipped with a police radio. The SPD used and intended to use Vehicle 2 in the same manner as Vehicle 1, both generally and during the protest on May 30, 2020. Vehicle 2 was parked on 6th Avenue between Pine Street and Olive Way, slightly behind Vehicle 1.

Vehicle 3: A 2009 Chevrolet Express Van owned by SPD and assigned to the South Precinct Anti-Crime Team. This van was not marked as a police vehicle, but was equipped with emergency lights and a police radio. The SPD used Vehicle 3 for the general purpose of transporting police officers and law enforcement equipment. During the protest, Vehicle 3 was parked on 6th Avenue between Pine Street and Olive Way, immediately behind Vehicle 2.

Vehicle 4: A 2016 Ford Explorer owned by SPD and used as a patrol car. Vehicle 4 was not marked, but was equipped with a push bumper, emergency lights, police radio, and other police equipment. During the protest, Vehicle 4 was parked on 6th Avenue between Pine Street and Olive Way, immediately behind Vehicle 3.

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Vehicle 5: A 2017 Ford Explorer owned by SPD and used as a patrol car. Vehicle 5 was not marked, but was equipped with a push bumper, emergency lights, police radio, and other police equipment. During the protest, Vehicle 5 was parked on Pine Street near 5th Avenue.

Vehicle 6: A 2016 Ford Explorer owned by SPD and used as a patrol car. Vehicle 6 was not marked, but was equipped with a push bumper, emergency lights, a police radio, and other police equipment. During the protest, Vehicle 6 was parked on 6th Avenue between Pine Street and Olive Way, directly behind Vehicle 4.

As described in detail below, during the protest on May 30, 2020, Vehicles 1, 2, 3, 4, and 5 were all damaged and destroyed by fire by multiple known and unknown suspects. Vehicle 6 was struck by an ignited incendiary device that then broke open on the adjacent sidewalk. After the arsons, investigators from SPD, FBI, and ATF examined the damaged vehicles. Vehicles 1, 3, 4, and 5 were completely destroyed by fire. Most of what remained were the metal frames of the vehicles. Vehicle 2 was also heavily damaged and is no longer operable, with the interior destroyed and the engine compartment burned. ATF Special Agent and Certified Fire Investigator Dawn Dodsworth examined these vehicles. She classified the fires in Vehicles 1, 3, 4, and 5 as "incendiary," meaning they were caused by human action. She further determined that the fire in Vehicle 2 was caused by the natural extension and expansion of the fire in Vehicle 1 into Vehicle 2.

The Seattle Police Department is involved in interstate and foreign commerce and in activities affecting interstate and foreign commerce.[1] The Seattle Police Department also is an institution and organization that receives Federal financial assistance. I have received

[1] *See United States v. Odom*, 252 F.3d 1289, 1294 (11th Cir. 2001) ("The legislative history of § 844(i) reveals that the statute was crafted specifically to include some non-business property such as police stations and churches.") (citing *Russell v. United States*, 471 U.S. 858, 860 (1985)); *United States v. Laton*, 352 F.3d 286, 300 (6th Cir. 2003) ("When it crafted § 844(i) to encompass the arson of police stations, Congress recognized that the provision of emergency services by municipalities can affect interstate commerce in the active sense of the phrase.") (citing *Jones v. United States*, 529 U.S. 848, 853 n.5 (2000); *Russell*, 471 U.S. at 860–61); *Belflower v. United States*, 129 F.3d 1459, 1462 (11th Cir.1997) (holding that § 844(i) covered the bombing of a police vehicle which a local sheriff's deputy used in his law enforcement responsibilities and that destruction of a police car had "a significant impact on interstate commerce" because the deputy patrolled traffic and made arrests on an interstate highway, issued citations to out-of-state drivers, participated in interstate narcotic investigations, assisted out-of-state authorities in apprehending suspects, recovered stolen property from other states, and attended law enforcement training sessions in other states).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

information from SPD's Chief Administration Officer, who oversees the SPD Grants and Contracts Unit, regarding the numerous federally funded grants SPD is currently receiving. In summary, SPD is presently receiving funding from a variety of federal agencies, including the Department of Justice, the Department of Homeland Security, and the Federal Emergency Management Agency (FEMA). Collectively, these grants total millions of dollars of federal funding provided to SPD in support of a variety of SPD's core duties and missions, including, but not limited to:

- Enhancing the safety of the community in the event of terrorist threats, active shooter threats, natural disasters, and the gathering of information helpful to law enforcement and the community regarding these sorts of serious threats;

- Providing crime prevention strategies and essential services to elderly, non-English speaking residents, refugees, deaf, blind and developmentally disabled residents of Seattle and working with communities to decrease crime by developing, implementing and coordinating crime prevention programs;

- Bolstering security measures related to the protection of the Port of Seattle;

- Funding the investigations of offenses involving acts of terrorism, chemical, radiological, or biological attacks, crimes against children, and human trafficking; and

- COVID Emergency Stimulus Funding used to pay for things such as personal protective equipment for officers; funding to backfill for officers testing positive for COVID or in quarantine; and the cost of providing protection for lives and property in the event of protests against statewide shelter-in-place orders or re-opening guidelines.

B. Kelly Jackson's Involvement in the Arsons of SPD Vehicles.

Investigators with SPD, FBI, and ATF have obtained and reviewed videos and photographs taken during the events surrounding the burning of the SPD vehicles on May 30, 2020. This video and photographic evidence came from various sources, including SPD personnel on scene, neighboring building surveillance cameras, footage aired by local

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

news media outlets, publicly reviewable social media posts, and from individuals who attended the protest and took their own photographs and video.

Based on these videos and photographs, FBI and ATF special agents have identified a male suspect who was involved in throwing at least two incendiary devices at the SPD vehicles. The suspect appears to be a white male with an athletic build. He was wearing a dark sweatshirt with a distinctive logo on the front, khaki pants, white shoes, a half-face respirator with black semi-rectangular filter cartridges, Smith ski goggles with black rims and yellow tinted lens, and a black High Sierra brand backpack. The white shoes appear to be consistent with the brand/style of Nike Air Force 1's.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Video footage shows that by approximately 4:06 p.m., Vehicle 5 was heavily damaged and burned by the actions of Margaret Aislinn Channon and other suspects who are currently unidentified. Immediately prior to that, at approximately 4:04 p.m., video footage shows the male suspect throwing what appears to be a glass bottle with an ignited fabric or paper wick (*i.e.*, a "Molotov cocktail" device) through the open driver's side door of Vehicle 5. After the bottle entered Vehicle 5, flames spread rapidly, almost instantaneously, through the passenger compartment. The spread was consistent with the rapid escape of a flammable liquid from a broken container. As the flames receded, a few areas of the interior of the vehicle continued to burn.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

At approximately 5:20 p.m., video footage shows the same male suspect throwing what appears to be a glass bottle with an ignited fabric or paper wick (another "Molotov cocktail") at the front of Vehicle 6. The device hit the windshield of Vehicle 6, bounced to the west, and then shattered on the sidewalk. After the bottle shattered, flames spread rapidly, almost instantaneously, across an approximately 12-foot radius along the sidewalk. The spread was consistent with the rapid escape of a flammable liquid from a broken container. After throwing the device, the male subject can be seen running north on 6th Avenue into a large crowd.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

On June 24, 2020, the Seattle FBI was forwarded an anonymous tip from the FBI's National Threat Operations Center. The anonymous reporter stated that they were providing information regarding the identity of an individual "using a 'Molotov' type device to set fire to [a] squad car" during the demonstrations in downtown Seattle on May 30, 2020. The tip specifically identified the above-referenced male suspect as Kelly Jackson of Edmonds, Washington. The anonymous reporter stated that they watched a video on a "peers [sic]" phone showing Jackson lighting a device and throwing it at a police vehicle. The anonymous reporter also stated that they heard that Jackson had been bragging about his activities amongst his friends who attended the protest. They described Jackson as wearing a "dark sweatshirt – khaki pants and also a gas mask" at the time of the arsons. The anonymous reporter further stated the gas mask was stolen from Jackson's employer, Jim Dandy Plumbing.

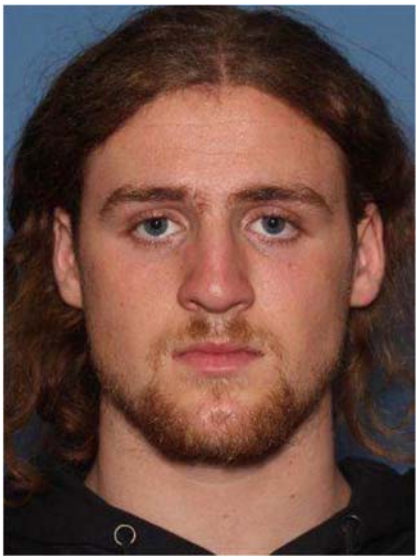
FBI agents determined that there is a Jim Dandy Sewer and Plumbing located at 6202 214th Ave SW, Mountlake Terrace, Washington. FBI agents reviewed Jim Dandy's website and Facebook page. On April 10, 2020, Jim Dandy Sewer and Plumbing posted a picture of an employee wearing company protective equipment. Agents observed that the

filter cartridges on the mask in the Facebook photograph appeared to be consistent with the filter cartridges on the mask worn by the male arson suspect on May 30, 2020. According to the Assistant Weapons of Mass Destruction Coordinator for the Seattle FBI, the respirator

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

shown in the Facebook photograph was a different model of half-face respirator than the male arson suspect wore, but would provide a consistent level of protection.

FBI agents queried the Washington Department of Licensing (DOL) and saw that Kelly Thomas Jackson has a Washington State driver's license. Jackson's residence address is listed with DOL as 21329 95th Avenue West, Edmonds, Washington. Agents reviewed



Jackson's DOL photograph. They saw it appeared consistent with the portion of the male arson suspect's face that was visible above his mask. Agents reviewed Jackson's criminal history and learned that he has been arrested in Snohomish County on prior occasions for, among other crimes, DUIs, resisting arrest, and burglary.

FBI agents individually interviewed three officers with the Edmonds Police Department. The officers were shown photos and videos of the male arson suspect on May 30, 2020. Each of the officers were unable to immediately identify the individual based on the images alone. However, when the agents informed the officers that the suspect was believed to live in Edmonds and had contact with them before, each officer stated that Kelly Jackson could be the suspect. All three officers explained that the suspect appeared consistent with the build, stature, and gait of Jackson. They also knew Jackson to be anti-law enforcement and believed the activities observed to be consistent with his past behavior.

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

FBI agents reviewed police reports and determined that Jackson typically operates a white 2002 Toyota Tacoma pickup truck, with Washington license plate C76599N. On June 24, 25, and 26, 2020, an FBI agent observed the Toyota Tacoma parked adjacent to Jim Dandy Sewer and Plumbing in Mountlake Terrace. The same FBI agent observed the Toyota Tacoma parked at Jackson's residence in Edmonds on June 24 and 25, 2020.

On July 2, 2020, agents observed a white male, believed to be Jackson, leaving his residence and driving the Toyota Tacoma. Jackson was wearing a dark hooded sweatshirt with a design on the front. This sweatshirt was consistent with the sweatshirt colors and logo worn by arson suspect on May 30, 2020.

Surveillance photo on July 2, 2020

Arsonist on May 30, 2020

Specifically, both sweatshirts are black with a small white mark on the left sleeve just above the wrist. The front of the sweatshirts have a design made up of three images and three words. The three images are side-by-side and evenly spaced. The left-most image is nearly the full height of the design, and the other images are roughly one-third to one-half the height of the design. The three images make up the left side, the bottom, and the left end of the top of the design. The remainder of the top and the right side of the design are made up of what appears to be three words in white text. The words are arranged in a vertical column, with one word per line.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

On July 3, 2020, agents again observed a white male, believed to be Jackson, leaving Jackson's residence and driving the Toyota Tacoma. The agents were able to see the driver of the vehicle from a very close distance, and the individual was not wearing a hat or mask. The agents positively identified the driver as Kelly Jackson, based on their familiarity with Jackson's DOL photo and prior booking photos of Jackson from the Snohomish County Jail.

C. Jackson's Possession and Use of a Phone during the May 30 Arsons.

FBI agents have reviewed numerous police reports documenting prior contacts between law enforcement officers and Jackson. Nine police reports list Jackson's phone number as (425) 892-0092. Subscriber records obtained from Verizon Wireless list the subscriber for this phone number as Maria Jackson, with the same residential address listed on Kelly Jackson's DOL records. Based on online research, I am aware that Maria Jackson is Kelly Jackson's mother. According to the Verizon Wireless records, telephone number (425) 892-0092 is associated with IMEI 354914090230305. This IMEI is assigned to an Apple iPhone 7 smartphone device ("the iPhone 7").

Based on this investigation, I believe that the arsonist on May 30, 2020, believed to be Jackson, possessed and used a smartphone during the time of the arsons; and specifically, that he possessed and used the iPhone 7 device. Multiple photographs and videos taken on May 30 show that the arsonist had an object in his pants pocket that was consistent with the size and shape of a smartphone.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

According to Verizon Wireless toll records, the iPhone 7 was used during and surrounding the time frame of the arsons. Between 3:00 p.m. and 6:00 p.m. on May 30, 2020, the iPhone 7 received 18 telephone calls for a total of approximately eleven minutes of use; and the iPhone 7 placed five phone calls for a total of approximately three minutes of use.

Based on this information, on July 31, 2020, the Honorable Chief Magistrate Judge Brian A. Tsuchida issued a search warrant directing Verizon Wireless to provide the FBI with cell-site and other locator data related to the iPhone 7, believed to be used by Kelly Jackson. *See* MJ20-488. On August 4, 2020, Verizon Wireless produced responsive records to the FBI relating to the time period of May 1, 2020, through June 30, 2020.

The Verizon Wireless records are consistent with Kelly Jackson being in downtown Seattle at the times and locations of the arsons on May 30, 2020. The records show that between 3:00 p.m. and 5:28 p.m. on May 30, 2020 (the time period of the arsons), the iPhone 7 was used to make calls while connected to cell towers located at the following addresses: (a) 1505 5th Avenue, Seattle; (b) 1200 5th Avenue, Seattle; (c) 1624 Boren Avenue, Seattle; (d) 810 Virginia Street, Seattle; (e) "1633 6th Avenue #3&4," Seattle; and (f) 1831 8th Avenue, Seattle. These cell towers are all located in the downtown Seattle core retail area. The recorded azimuth data from the towers is consistent with the iPhone 7 being located within the core retail area from approximately 3:36 p.m. until approximately 5:28 p.m. on May 30, 2020. As discussed previously in this affidavit, the arson suspect threw at least two incendiary devices within the core retail area, one at approximately 4:04 p.m. and one at approximately 5:20 p.m.

Notably, during the two month timeframe covered by the records provided by Verizon Wireless, the only day on which the iPhone 7 connected with any of the above mentioned cell towers was May 30, 2020. During the remainder of the time period, the iPhone 7 never otherwise came within two miles of the cell towers in the downtown Seattle retail core.

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

D. Description of Kelly Jackson's iCloud Account.

There is probable cause to believe that the Apple iCloud account registered to the email address yaherd300@gmail.com belongs to Kelly Jackson and will contain evidence of the Arson crimes under investigation. Records produced by Apple show that an iCloud account bearing digital sign identifier 16913302770 was created in 2019 and was registered under the name Kelly Jackson, the email address yaherd300@gmail.com, the residential address 21329 95th Avenue West, Edmonds, Washington, and the phone number (425) 892-0092. This residential address is the same address listed on Jackson's driver's license and is the address at which agents have observed Jackson coming and going. The phone number is the same phone number that is tied to Jackson as described above.

1. The Apple records also show that:

a. Since its creation, the SUBJECT ACCOUNT had activated, and used, the following Apple iCloud features: iCloud Backup (iOS Devices), iCloud Drive, iCloud Photos, Calendars, Bookmarks, and Notes.

b. The SUBJECT ACCOUNT is in "active" status.

c. The user of the SUBJECT ACCOUNT has used at least one device in connection with the SUBJECT ACCOUNT, including an iPhone 7. The SUBJECT ACCOUNT's user most recently registered an iPhone 7 in October, 2019.

d. The SUBJECT ACCOUNT has regularly engaged in activity which Apple has "logged." For instance, the SUBJECT ACCOUNT's activity logs show that data has been "backed up" from the user's device to the SUBJECT ACCOUNT's cloud-storage capabilities multiple times between July 20, 2020, and July 29, 2020. Apple records show other logged activity involving the SUBJECT ACCOUNT, including that the Find my iPhone (FMIP) and Calendars applications were logged between July 14, 2020, and July 29, 2020. Of note, the logs reference a device type of "D10AP" and "iPhone9,1," both of which refer to the iPhone 7 model device, according to my open source research.

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

BACKGROUND REGARDING APPLE ID AND iCLOUD[2]

Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system

Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive

[2] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. For instance, evidence that identifies the user of an Apple iCloud account at the time that the phone connected to that account engaged in a WhatsApp chat (or sent an email) can establish a direct connection between the phone's user and the incriminating chat (or email).

Further, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to document, discuss, and otherwise communicate about and/or facilitate the offenses under investigation. In this case, there is probable cause to believe that Kelly Jackson possessed the above-referenced iPhone 7 device during the arsons on May 30, 2020, and that he used the device throughout the time period of the arsons. Moreover, the above-referenced anonymous reporter stated that they watched a video on a peer's phone showing Jackson lighting a device and throwing it at a police vehicle. The anonymous reporter further stated that they heard Jackson had been bragging about his activities amongst his friends who attended the protest. This information indicates that Jackson likely possessed and shared video or photographic evidence of the arsons, and otherwise communicated about the arsons, using the iPhone 7, and that therefore this information may also be stored in the SUBJECT ACCOUNT.

In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

//

//

//

//

//

//

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

CONCLUSION

Based on the forgoing, there is probable cause to believe that evidence of violations of Arson, in violation of Title 18, United States Code, Sections 844(f)(1) and (i), will be found in the SUBJECT ACCOUNT, as more fully described in Attachment A. I therefore request that the Court issue a warrant authorizing a search of the SUBJECT ACCOUNT for the items more fully described in Attachment B, and the seizure of any such items authorized therein. Because the warrant will be served on Apple, which will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

NATHAN PLOUGH, Affiant
Special Agent, FBI

The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit on the 11th day of August, 2020.

MARY ALICE THEILER
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970